Carnegie UK Trust response to ICO consultation on Age Appropriate Design: a code of practice for online services

1. We welcome the publication of the Code by the ICO. As the authors of Carnegie UK Trust's detailed proposal for a statutory duty of care to reduce harm on social media[1], which has informed the Government's recent proposals in its Online Harms White Paper, we commend the Code as an important first step in moving towards a system-level approach to addressing digital harms that is proactive, precautionary and proportionate. We are also supportive of the role that 5 Rights Foundation has had in influencing the development of the code and in the detailed points that they have raised with us and other stakeholders during the consultation period, which will be reflected in their formal response.

2. We are responding to this consultation from the perspective of our interest in the wider online harm reduction agenda and the implementation of a statutory duty of care, as set out in the recent Government Online Harms White Paper. As such, we do not have specific detail to provide on every aspect of the consultation's questions but have focused on some areas which we feel are particularly notable.

3. As we set out in our work, computer code sets the conditions on which the internet is used; code is the architecture of cyberspace and this, combined with business decisions (such as those that shape the collection and use of personal data) affects what people do online. It is becoming increasingly apparent that the architecture and design of the platform – as formed by code - also nudges us towards certain behaviour, whether this is the intention of the software designer or not. Even where not designing in features (such as 'likes' or recommendations) which are designed to keep users engaged, there is a concern that when a developer is focussed a particular objective, they may also overlook other interests and possible side-effects of design choices. The environment within which harm occurs is defined by code that the service providers have actively chosen to deploy, their terms of service or contract with the user and the resources service providers deploy to enforce that.

4. We observe in our work that, if services providers chose to prioritise the reduction of online harm to vulnerable users, they "could choose not to deploy risky services without

[1] See our full detailed paper (April 2019) along with our original blog posts and other materials here: https://www.carnegieuktrust.org.uk/project/harm-reduction-in-social-media/

safeguards or they could develop effective tools to influence risk of harm if they choose to deploy them." The same is true of data protection and protecting children's privacy. Service providers can deploy tools to prioritise the safeguarding of children's rights. The Age Appropriate Design Code (AADC) sets out clearly what these choices look like.

5. The 'by design' approach on which the AADC is based is an effective mechanism draw attention to the fact children's data rights and privacy can *and should* be taken into account in service design, not bolted on as an afterthought. The implementation of this Code is an acknowledgement that, up to this point, those choices have not – in general – been made voluntarily by service providers. Regulation and codes of practice therefore become necessary to deliver system change; in this regard, we see the ICO's code as an important forerunner of the wider regulatory system, underpinned by codes of practice, that is envisaged in the DCMS Online Harms White Paper.[2] The ICO's code has the potential to be transformative in the protection of children's rights online – and we urge the ICO to ensure that its design, and the interconnectedness of the standards, as set out in the consultation version is implemented in its totality.

6. We set out below some specific observations and comments on the consultation questions on the proposed standards, particularly with regard to the wider Online Harms policy agenda and synergies with our work on the design of a statutory duty of care.

Services in scope

7. We feel that this is communicated clearly in so far as it explains the definition of "relevant information society services (ISS)" and we recognise that this is the terminology that is used in the Data Protection Act and, as such, is widely recognised. We would make the point, however, that there is no equivalent definition used in the DCMS Online Harms White Paper, which focuses instead on listing types of services that "allow users to share or discover user-generated content or interact with each other online". There will therefore be an overlap between the sub-set of information society services covered by the duty of care legislation and those caught under the Code's "ISS" definition.

8. The overarching aims of the White Paper's statutory "duty of care" are wider than those of the Age Appropriate Design Code, yet the scope of services it covers appears to be narrower. The White Paper says that "we expect the framework will be complementary with existing privacy by design and security by design standards. For example, it will reflect and signpost the forthcoming Age-appropriate Design Code and the Code of Practice for Consumer Internet of Things Security." As stated above, we see the Age Appropriate Design Code as potentially being an exemplar for how the codes of practice envisaged under the Duty of Care might be designed so that they effectively help to reduce the risk of reasonably foreseeable harm occurring to users of services: that is, being systemic, risk-based, proportionate and flexible. While not for the ICO to address in response to this

[2] Our detailed view on the proposals in the White Paper, particularly the differences between the "duty of code" regime that we envisaged and that described by the Government, will be published soon.

consultation, we raise the risk here – and will also do so in our response not the Online Harms White Paper – of the potential for inconsistencies in scope (and potential challenges for regulators in responding to it) where there are overlapping codes within the wider statutory duty of care framework.

Standards of age appropriate design

1) Best interests of the child

9. We have submitted a response to the recent consultation on the UN Convention on the Rights of the Child (UNCRC) general comment on the rights of the child in a digital age[3]. This submission sets out how a statutory duty of care can deliver many of the safeguards required such that online services are designed and delivered in the best interests of the child.

2) Age-appropriate application

10. We note that the age verification requirements are central to the AADC but it is important to stress that this is not the only element that will have impact. Age verification could also be an important part of a raft of system level approaches that companies could follow in order to meet their wider harm reduction obligations to children under the statutory duty of care. If companies cannot prove that they know the age of the users of their services, then they are not able – as proposed in the duty of care – to minimise the reasonably foreseeable risk of harm to children using those services, whether that is through accessing or being recommended inappropriate or harmful material or being vulnerable to exploitation by adults.

11. We note that the code states that "You must not use data collected for age-verification purposes for any other purpose" but we feel that this should have heavier emphasis; there is a strong principle already in existence, as set out in the Audio Visual Media Services Directive, and the ICO may wish to make reference to this.

12. We recognise that age verification technology is a fast-evolving area; it is also one that, as demonstrated by the response to the introduction of age verification to restrict under-age access to porngraphy, is not without controversy, carrying a risk of unintended harms arising from the mass collection of personal data to verify identity. So we support the commitment that is made in the Code that the Information Commissioner will "support work to establish clear industry standards and certification schemes to assist children, parents and online services in identifying robust age-verification services which comply with data protection standards". This will also be important to ensure that this requirement doesn't create a barrier to entry to small, or new, firms. We see the statutory duty of care applying regardless of the size or relative newness of a social media company,

[3] Our response here: https://www.carnegieuktrust.org.uk/publications/response-to-un-committee-on-the-rights-of-the-child-uncrc-consultation-on-the-concept-note-for-a-general-comment-on-childrens-rights-in-relation-to-the-digital-environment/

but that the regulator's enforcement should be proportionate; a similar consideration may need to be taken here while the market in age verification technology evolves.

4) Detrimental use of data

13. We welcome the focus here on mitigating the risk that the use of children's data, particularly to fuel strategies to extend user engagement, can be detrimental to their wellbeing. We also welcome the references to the UK Chief Medical Officers' advice that a "precautionary approach" is necessary in lieu of further research on the impact of social media use on the health and wellbeing of children. Our Carnegie work sets out how the adoption of the "precautionary principle", an approach well-established in UK policymaking when faced with threats to public health but before scientific certainty can be reached, is an important foundation for a risk-based statutory duty of care.

14. One of the recurrent arguments put forward for not regulating social media and other online companies is that they are unique or special: a complex, fast-moving area where traditional regulatory approaches will be blunt instruments that stifle innovation and require platform operators to take on the role of police and/or censors. Another is that the technology is so new, sufficient evidence has not yet been gathered to provide a reliable foundation for legislation; where there is a body of evidence of harm, in most cases the best it can do - as found by the Chief Medical Officers - is prove a correlation between social media use and the identified harm, but not causation.

15. Our work consistently argues that the traditional approach of not regulating innovative technologies needs to be balanced with acting where there is good indicative evidence of harm, but where full scientific proof has not yet been attained. We are concerned that some cynical actors might seek to manipulate an evidence process by suggesting that constantly changing software (a feature of modern web services using continuous push deployment) cannot be subject to traditional long-term randomised control trials. The software constantly changes so you cannot set a fixed point against which to measure. The precautionary principle provides for cautious action by companies, rather than banning. It requires companies to accept that they bear the burden of providing what evidence they have for public scrutiny by regulators and civil society. After the science-public opinion debacles of the 1990s the Cabinet Office set out in 2002 an inter-departmentally agreed, risk-managed approach to the precautionary principle that remains in force today. [4]

16. The Age Appropriate Design Code is an excellent example of how that "need to act" can be translated into clear, practical steps for companies to integrate into the design stage for new services and products, and by which they can prove to regulatory bodies that they have done everything reasonable to reduce harm.

[4] http://www.hse.gov.uk/aboutus/meetings/committees/ilgra/pppa.htm

6) Default settings

17. This is an important provision and one which corresponds to the principles that underpin the statutory duty of care and its particular application to children. We believe that service providers should design their services in a way that reduces the risk of reasonably foreseeable harm to all users, and with particular consideration where appropriate for vulnerable groups. If we use the analogy of the online world as being akin to a public space, if an owner of a theme park was to leave it to children visiting their park to protect themselves from harm without designing in default safety measures, they would not be fulfilling their responsibility under well established duty of care legislation. The same should be true online; so, where a mass membership, general purpose service is open to children and adults, it should manage risk by setting a very low tolerance for harmful behaviour, in the same way that many public spaces take into account that they should be a reasonably safe space for all ages. The same is true for data protection and privacy in relation to children's use of services.

18. For many services covered by the Age Appropriate Design Code, this demonstrates why robust age verification mechanisms are required and is an example of how the various standards in the code are interdependent: without being able to determine the make up of its user base (for example, whether it is used by the general population, including children, or primarily by adults) then, any service collecting data would need to apply child-appropriate default settings. We welcome this as a ground-breaking means by which to design in safety for all users of online services and one which would fit neatly underneath the proposed statutory duty of care for wider harm reduction objectives.

9) Geolocation

19. When considered under a statutory duty of care framework, the use of geolocation data from children without consent is another important example of how the principle of harm reduction applies equally online as well as offline – and where decisions made in an online environment (eg to track or record children's location or movements via an online service) can raise the risk of serious harm in the physical world. We therefore welcome the fact that the Code acknowledges this risk, as well as the fact that using geolocation services can undermine a number of the rights of the child, and puts the onus on the service provider to turn geolocation data off by default. We concur with the position taken by 5 Rights Foundation that, in order to fully deliver on the intent of the Code, children should not be nudged to activate geolcation services except for the specific purposes intended.

11) Profiling

20. In terms of wider harm reduction under a duty of care, particularly the targeting of harmful content to vulnerable groups, we welcome the means by which the Code translates the requirement under Recital 38 of GDPR for special protection for children into practical design requirements for service providers to meet this. In this area, we also agree with 5 Rights' view that the Code should explicilty prevent online services from

profiling children unless there is a compelling reason to do so, having regard to the best interests of the child; and that, where profiling is deemed to be in the best interest of the child, the Code should make clear that its intention is to prevent online services from profiling children either in more detail than is necessary to provide them with the service or feature they are actively and knowingly engaged with, or for purposes that are not necessary to provide that service or feature.

21. We particularly welcome the very clear statement of responsibility that service providers have for the recommendations that flow from their profiling of users: "*if you are using children's personal data to automatically recommend content to them based on their past usage/browsing history then you have a responsibility for the recommendations you make. This applies even if the content itself is user-generated*." This point has particular relevance to the wider principle of a Duty of Care; we set out in our work how the Duty would cover all aspects of the design of services which impact on the user; recommender algorithms would be included in this, particularly given that significant concern has been raised about the intent behind their design and its impact on users.[5]

22. We also applaud the Code's success in setting out clearly how the precautionary principle should work in practice, in a context where harms emerge and evolve quickly: "*your general approach should be that if the content you promote or the behaviours your features encourage are obviously detrimental, or are recognised as harmful to the child in one context (eg marketing rules, film classification, advice from official Government sources such as the Chief Medical Officer's advice, PEGI ratings) then you should assume that the same type of content or behaviour will be harmful in other contexts as well*." We are pleased to note that "*user-generated content .. that is obviously detrimental to children's wellbeing or is formally recognised as such (eg pro-suicide, pro-self harm, pro anoriexia content)*" is included as an example of the type of content to be considered. We would also include in this a particular responsibility to children in relation to the range of reliable information that they are provided with on any given topic. We hope that the development of the subsequent Codes of practice to underpin the Duty of Care will follow this model in cases where evidence or specificity of harm is not readily available within an online context.

12) Nudge techniques

23. We welcome the groundbreaking provisions in the Code to address nudge techniques and other “persuasive design” elements of online services that aim to keep children engaged and active online for as long as possible. Nudge techniques are not just a concern in relation to providing content to children, but also in encouraging them to share personal data and communicate information about themselves online. We have set out above how our work to develop a duty of care proposal is predicated on the fact that companies are

[5] Anthropological research suggests that those coding recommender algorithms see their function as ‘hooking’ users; that these algorithms operate as a trap: N. Seaver, ‘Captivating algorithms: Recommender systems as traps’ (2018) Journal of Material Culture: https://journals.sagepub.com/doi/10.1177/1359183518820366

responsible for every element of the design and functioning of the services they operate. For many, these services were deliberately designed to keep people's attention. Sean Parker, a co-founder of Facebook said in a 2017 interview: 'God only knows what it's doing to our children's brains. The thought process that went into building these applications, Facebook being the first of them, ... was all about: How do we consume as much of your time and conscious attention as possible?.... It's a social-validation feedback loop ... exactly the kind of thing that a hacker like myself would come up with, because you're exploiting a vulnerability in human psychology.'[6]

24. By including nudge techniques in the Code, the ICO is addressing one of the fundamental choices that online businesses make when designing their services; and setting down a clear marker that the types of tactics used to keep adults engaged are not necessarily appropriate to children. In the absence of robust evidence in this area – whether on the impact of "screen time" on the health and wellbeing of children, or on the nature and consequences of excessive use to social media, or the introduction of elements of gambling (such as loot boxes) in online gaming – taking a precautionary approach is absolutely key to reducing the risk of foreseeable harm to vulnerable groups.

25. We know that this particular standard is likely to be contentious and attract opposition from many of the services likely to be covered by the code – and we also acknowledge that there are many positive uses of nudge techniques that can be deployed to improve the online experience for users and to mitigate the risk of harm. However, we fully support the intention that this standard will prohibit nudge or other persuasive design techniques that are *intended* to keep children online for as long as possible.

13) Connected toys and other devices

26. We welcome the inclusion of connected toys and other devices in the Code, particularly given the fact that, as more and more devices and home appliances become "smart" or connected to the Internet of Things, the risks to children's privacy and the protection of their personal data will increase. We welcome the fact that the Code specifically deals with smart speakers and other connected devices that may be used by children, along with other members of a family or household group. We have not specifically covered connected devices in our proposals for a duty of care but welcome the incorporation of a "by design" approach - not just into this ICO code but also into the DCMS "secure by design" code[7] for IoT, which is also out for consultation at present. It will be important that these two codes are aligned so that the services that fall in scope for both of them have consistency and clarity on the design considerations to which they have to comply.

---

[6] Article: 'Sean Parker unloads on Facebook: "God only knows what it's doing to our children's brains"' Axios, Mike Allen Nov 9, 2017 https://www.axios.com/sean-parker-unloads-on-facebookgod-only-knows-what-its-doing-to-our-childrens-brains-1513306792-f855e7b4-4e99-4d60-8d51- 2775559c2671.html; more recent journalism suggests that YouTube also ignored risks to users or to the information environment in the search for engagement: M. Bergen, 'YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant' Bloombeg, 2 April 2019, available: https:// www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-lettingtoxic-videos-run-rampant (accessed 3 April 2019)

[7] https://www.gov.uk/government/collections/secure-by-design

27. One area that does not appear to be covered in the Code are apps or other software that collect data – whether personal or inferred – that is about children, often for use by parents or educational settings to monitor or review aspects of their activity.

15&16) Data protection impact and assessments; and governance and accountability

28. These two sections are, we feel, important in setting out the types of due diligence and monitoring/governance of impact required in any "by design" or "duty of care" framework to mitigate risks of harm to users of online services. For either such approach to work, they have to be implemented at a system level and integrated into a company's corporate decision-making and accountability processes. The evidence that will be recorded under both standards is vital not just for compliance with regulatory or statutory duties but also for transparency purposes and to identify evidence of impact. Again, we see the approach set out here as setting a helpful standard by which the design of the Government's wider regulatory system to reduce online harms can judged, and into which it should be integrated in due course.

29. We hope that these comments are helpful and look forward to the swift implementation of the Age-Appropriate Design Code after this consultation has closed.

Professor Lorna Woods

William Perrin

Maeve Walsh

May 2019

Contact: [redacted]